UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/293,142	04/16/1999	TAKASHI KONDOH	990242LH	4480

7590 08/28/2003

FRISHAUF HOLTZ GOODMAN
767 THIRD AVENUE 25TH FLOOR
NEW YORK, NY 100172023

EXAMINER
MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 08/28/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/293,142	KONDOH ET AL.	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. Claims 1-27 are pending.

2. The applicant has amended to overcome 112 rejections.

Response to Arguments

3. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-3 are rejected under 35 U.S.C. 102(b) as being anticipated by Friedman U.S. Patent No. 5,499,294.

As to claim 1, Friedman discloses a camera including an image pickup unit for picking up an image of an object [figure 3a]. Friedman discloses an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit [figure 3b]. Friedman discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption

processing unit using a decryption key corresponding to the encryption key [figure 3c]. Friedman discloses detecting whether the image data has been altered based on a result of the decryption [column 6, lines 30-52]. Friedman discloses that the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer [column 6, lines 2-29].

As to claim 2, Friedman discloses that the encryption processing unit also utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [column 7, lines 18-45].

As to claim 3, Friedman discloses that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [column 6, lines 2-29].

5. Claims 4-7, 14, 16 and 19-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Squilla et al U.S. Patent No. 5,898,779.

As to claims 4-6, 14 and 16, Squilla et al discloses a camera including an image pickup unit for picking up an image of an object [figure 2]. Squilla et al discloses encryption processing unit for generating alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit [figure 2]. Squilla et al discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key [figure 6]. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption [figure 6]. Squilla et al discloses that the encryption processing unit generates the alteration detection data based on the encryption key, the image data, and data for identifying a photographer [figure 5]. Squilla et al discloses that the encryption processing unit generates first data from the image data using the encryption key, generates second data from the image data using the data for identifying the photographer, and combines the first data and the second data into the alteration detection data [figure 5]. Squilla et al suggests that the second encryption processing unit is removably mounted on the camera [figure 2]. Squilla et al discloses that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined

and stored in different sets [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the encryption processing unit includes a selection unit for selecting at least one image data having a desired resolution from the multiple resolution image data in order to generate the alteration detection data [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that each of the multiple resolution image data is stored in units of a predetermined small block [column 8 line 52 to column 9 lines 15]. Squilla et al discloses that the encryption processing unit generates the alteration detection data in units of the small block [column 8 line 52 to column 9 lines 15].

As to claim 7, Squilla et al discloses that the encryption processing unit generates the alteration detection data using the encryption key from a combination of the image data and the data for identifying the photographer [figure 5].

As to claims19, 21 and 23, Squilla et al discloses that the encryption processing unit also utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [figure 5].

As to claims 20, 22 and 24, Squilla et al discloses that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [figure 6].

6. Claims 9, 12 and 13 are rejected under 35 U.S.C. 102(b) as being anticipated by Moore U.S. Patent No. 5,343,527.

As to claim 9, Moore discloses a decryption key server including a decryption key storage unit for storing a unique identifier to the system and a first decryption key corresponding to a first encryption key generated as a key corresponding to the identifier [figure 2A]. Moore discloses a decryption key output unit for generating alteration detection data for the first decryption key using the second encryption key and outputting the alteration detection data together with the first decryption key [figure 4]. Moore discloses a decryption key

acquisition unit including a decryption key storage unit for storing the first decryption key acquired from the decryption key server through communication means [figure 6]. Moore discloses an alteration detection unit for decrypting, using a second decryption key corresponding to the second encryption key, the alteration detection data supplied from the decryption key server through the communication means and detecting whether the first decryption key has been altered based on a result of the decryption [figure 7].

As to claim 12, Moore discloses that the editing history data is recorded in combination with the information for user authentication [figure 4].

As to claim13, Moore discloses that the image data is stored in an external medium, and the image input unit inputs the image data from the external storage medium by connecting directly to the image filing unit or through a communication line [figure 8].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Steinberg U.S. Patent No. 5,862,218.

As to claim 8, Squilla et al discloses a camera including an image pickup unit for picking up an image of the object. Squilla et al discloses an encryption processing unit for generating alteration detection data using a built-in encryption key from the image data obtained by the image pickup unit. Squilla et al discloses an alteration detection unit for decrypting the alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption, all discussed above. Squilla et al discloses that the camera includes a mode selection unit for selecting at least one of an alteration monitor mode for detecting whether the image data has been altered. Squilla et al discloses a secure mode for encrypting the image data

transferred from the camera to the alteration detection unit, all as discussed above. Squilla et al suggests a normal mode for taking a photograph without a security function [figure 2].

Squilla et al does not teach a digital watermark mode for embedding a digital watermark in the image data.

Steinberg teaches a digital camera with a digital watermark mode for embedding a digital watermark in the image data [abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that one of the modes as taught would have included a digital watermark mode for embedding a digital watermark in the image data.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Steinberg because it provides a marked, secure images that minimizes concerns regarding unauthorized use [column 2 line 15 to column 3 line 3].

8. Claims 10, 11, 15, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Smith et al U.S. Patent No. 5,329,623.

As to claim 10, Squilla et al discloses a filing management unit for filing and managing the image data input thereto through an image input unit. Squilla et al discloses an alteration detection unit for decrypting first alteration detection data attached to the image data by use of a decryption key corresponding to a first encryption key used for generating the alteration detection data. Squilla et al discloses comparing the first alteration detection data thus decrypted with the image data thereby to detect the alteration of the image data. Squilla et al discloses an image editing unit for processing the image data and an image file updating unit for generating second alteration detection data, all as discussed above.

Squilla et al does not teach using a second encryption key other than the first encryption key from the image data processed by the image editing unit and editing history data output by the image editing unit, and for adding the second alteration detection data to the edited image data.

Smith et al teaches an encryption chip that generates multiple keys [column 3, lines 18-26].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that the second alteration data would have been generated by using the multiple keys provided by Smith et al.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Steinberg because any application can employ the encryption hardware, for example, to encrypt and decrypt data written to disk, or to provide application-to-application cryptographic support [column 8, lines 18-35].

As to claim 11, the Squilla-Smith combination suggests that the image file updating unit is removably mounted on the digital image editing system and has stored therein information for user authentication information and the second encryption key [Squilla figure 2]. The Squilla-Smith combination teaches that the second alteration detection data is generated using the second encryption key and the information for user authentication [Smith figure 7].

As to claim 15, the Squilla-Smith combination teaches that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets [Squilla column 8 line 52 to column 9 lines 15]. The Squilla-Smith combination teaches that the encryption processing unit includes a selection unit for selecting at least an image data having a desired resolution from the multiple resolution image data in order to generate the alteration detection data [Squilla column 8 line 52 to column 9 lines 15].

As to claim 17, the Squilla-Smith combination teaches that the image data comprises multiple resolution image data including a plurality of image data of different resolutions combined and stored in different sets, as discussed above. The Squilla-Smith combination teaches that each of the multiple resolution image data is stored in units of a predetermined small block and the encryption processing unit generates the alteration detection data in units of the small block, as discussed above.

As to claim 18, the Squilla-Smith combination suggests that at least a part of the image file updating unit is removably mounted on the digital image editing system [Squilla figure 2] and has stored therein editor

information and. the second encryption key [Smith figure 7]. The Squilla-Smith combination teaches that the second alteration detection data is generated using the second encryption key based on the image data and data obtained by applying a predetermined function from the editing history data output by the image editing unit [i.e. hashing function].

9. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Squilla et al U.S. Patent No. 5,898,779 in view of Hamada et al U.S. Patent No. 5,185,798.

As to claim 25, Squilla et al discloses a camera including an image pickup unit for picking up an image of an object. Squilla et al discloses a first encryption processing unit for generating first alteration detection data using a built-in encryption key from the image data picked up by the image pickup unit. Squilla et al discloses an alteration detection unit for decrypting the first alteration detection data generated by the encryption processing unit using a decryption key corresponding to the encryption key. Squilla et al discloses detecting whether the image data has been altered based on a result of the decryption. Squilla et al discloses a storage unit for storing data for identifying a photographer and the encryption key. Squilla et al discloses a second encryption processing unit for generating second alteration detection data from the data for identifying the photographer, all as discussed above.

Squilla et al does not teach that the second encryption processing unit is removably mounted on the camera.

Hamada et al teaches an IC card that includes an encrypting circuit [abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al so that the images would have been stored on the IC card. The IC card would have been removable from the camera.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Squilla et al by the teaching of Hamada et al because even if the data is tampered with, identification can be made, upon request by the IC card owner, on the card issuing person's side, whether or not the data in the magnetic or optical recording area is tampered with [column 5, lines 20-25].

As to claim 26, the Squilla-Hamada combination teaches that the encryption processing unit utilizes data obtained by application of a predetermined function to the image data to generate the alteration detection data [i.e. hashing function].

As to claim 27, the Squilla-Hamada combination teaches that the alteration detection unit detects whether or not the image data has been altered by comparing the data obtained by application of the predetermined function to the image data with data obtained by decrypting the alteration detection data using the decryption key [Squilla figure 6].

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-1373.

Aravind K Moorthy

August 18, 2003

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100